REMARKS

Claims 1, 13-15, and 17-21 are pending in the present application. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Claims 1, 13-15 and 17-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Griffin et al. (U.S. Patent No. 5,249,294) in view of Kocher et al. (U.S. Patent Publication No. 2002/0124178). This rejection is respectfully traversed for the following reasons.

Claim 1 recites method for securing a computer system which comprises at least a code interpretation module and memory capacities for storing an interpreted code having measurable physical imprints, wherein in order to make more difficult attacks based on physical measurements or requiring synchronization with the interpreted code, the method comprises the steps of providing at least two different implementations for at least one instruction of the interpreted code, the different implementations each requiring a different execution time and/or having a different physical imprint while providing an identical result, selecting one of the different implementations to be executed before each execution of the instruction, and executing the determined different implementation of the at least one instruction. This is not taught, disclosed or made obvious by the prior art of record.

The Office Action asserts that the sole difference existing between Applicants' method as claimed in claim 1 and Griffin resides in the fact that Griffin does not

recite explicitly that the system comprises a code interpretation module. In this respect, the Examiner refers to the specification text of Griffin, mainly in the chapter "Background of the Invention," which states, at column 1 lines 15-29:

> A clock attack is a procedure by which an attacker gains access to secure data or code used in a predetermined data processing continue being executed within a secure data processor, such as a secure microprocessor, by determining the time of execution, of the predetermined data processing routine in relation to occurrence of an externally observable event that proceeds the predetermined routine in order to enable synchronization with an internally generated instruction for the predetermined routine, and then externally changing the clock cycle for one cycle of the instruction in order to create a very short clock cycle that alters the instruction in a repeatable way that makes the secure data and/or code externally accessible.

Applicants respectfully submit that the teaching of this paragraph only refers to the definition of a clock attack and not to a solution to abort such an attack.

The Office Action also cites column 1, lines 30-34, which states:

> An "externally observable event" is defined as any internal state transition that manifests itself externally including but not limited to a change in voltage or current at any pin or combination of pins which is related to or affected by internal processor execution.

This paragraph only gives the definition of an "externally observable event" but not a solution to prevent use of such an event by an attacker to access to secure data or code.

The Examiner also refers to the chapter "Summary of the Invention," which defines the Griffin's invention and which states that (at column 1, lines 45 to 49):

> The method of the present invention includes the steps of (a) randomly varying the duration between the occurrence of the externally observable event and the execution of the predetermined routine [which follows the occurrence of the externally observable event].

This step, in which the duration is varied randomly, does not correspond to the method claimed in Applicants' claim 1.

More particularly, the cited paragraph, lines 45 to 49, does not mean that two different implementations are provided for at least one instruction of an interpreted code and that one of these two implementations is selected to be executed before each execution of said instruction.

The Office Action also cites column 1, lines 61-62, which states that:

> For this step of the invention, steps (b) and (c) preferably include the step of (d) randomly assembling m said interim routines for said execution from a group of n stored countries having different durations.

However, Applicant's method does not use any interim routine which is executed in the period between the occurrence of an externally observable event and the execution of a predetermined routine. In addition, Applicants' method does not comprise a step of randomly assembling the interim routine from a group of stored routines having different durations: the use of such a teaching cannot lead to Applicants' solution, which proposes to execute a different implementation of one instruction, and not to add an interim routine as described in Griffin.

The Office Action also cites Figure 1, as allegedly showing executing routines/instructions by a processor. Applicants respectfully submit that this figure makes more apparent the fact that the branch routine 12 causes the CPU 10 to branch to the maze of an interim routines and that the branch routine 12 saves the address of the instruction for the protected routine W in a secure memory location, which is only accessed

after execution after of the maze of interim routines 20, 21, 22 is completed. This method does not correspond at all to Applicants' claimed method.

For the reasons set up above it clearly appears that the difference between Griffins' solution and Applicants' solution is not limited to only the use of a code interpretation module and that Applicants' solution cannot be obviously deduced from the Griffin's teaching.

As stated in the reply to the Office action of January 07, 2008, Kocher discloses several known techniques used for protecting cryptosystems. However none of these techniques corresponds to the method as claimed in Applicants' claim 1.

On paragraph [0058] line 20 Kocher states that:

> Because a phase locked loop can produce an internal clock signal that is a multiple of the external clock signal it is possible to clock cryptographic operations at a rate faster than the external clock, providing improved performance. In smartcards with challenging performance requirements (such as those that run interpreted codes such as Java)...".

It clearly appears that Applicants' solution does not comprise anything similar to a locked loop or a means to clock operations at a rate faster than the external clock. Further, this teaching cannot lead to Applicants' invention even if one of ordinary skill in the art would have been motivated to combine it with Griffin (the obviousness of which Applicants contest).

For at least this reason, the proposed combination of Griffin and Kocher would not have rendered claim 1 obvious, as well as claims 13-15 and 17-21, which depend from claim 1. For at least these reasons, Applicant respectfully submits that claims 1, 13-15

and 17-21 are patentable over the prior art of record whether taken alone or in combination as proposed in the Office Action.

In view of the above amendment and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to the effect is most earnestly solicited.

If the Examiner has any questions, he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:me
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
C:\Users\Public\Documents\BN\Moutard\Hameau2\2008-12-15Amendment.doc